CLAIMS

1. A process to identify a user terminal resource (TU, CP; PC, CA) or a user of the terminal resource by a server resource (MS; SE) through such a telecommunication network (RR; RT), using a first identifier (ID), where an asymmetrical algorithm (AA) with public key (KPU) is implemented in the terminal resource, characterised by:

- the generation (E1, E21) of a random number (R) in the user terminal resource (TU, CP; PC, CA) ,

- the determination (E4, E5; E25) in the terminal resource of a second identifier (IA1; IA2) as a function of the random number (R), at least from part of the first identifier (ID) and from the result of executing the asymmetrical algorithm (AA) to which at least the random number is applied,

- transmission (E6; E26) of the second identifier (IA1; IA2) to the server resource (MS; SE), and

- in the server resource, retrieval (E9, E10; E29) of the first identifier (ID) at least by executing the asymmetrical algorithm (AA) to which a private key (KPR) and, at least partially, the second identifier (IA1; IA2) are applied, so that the server resource verifies that the first retrieved identifier (ID) is written into a memory (HLR) of the server resource.

2. A process according to claim 1, in which the steps described in claim 1 precede at least one authentication (E13) of the terminal resource (TU, CP; PC, CA) by the server resource (MS; SE).

3. A process according to claim 1 or 2, in which the determination in the terminal resource (TU, CP; PC, CA) includes application (E4) of the generated random number (R) to the asymmetrical algorithm (AA) with the public key (KPU) to produce an encrypted random number (RC), application (E5) of the generated random number (R) as a key, and of the first identifier (ID), to a symmetrical algorithm (AS) implemented in the terminal resource, to produce an encrypted identifier (IC), and concatenation (E6) of the encrypted random number (RC) and of the encrypted identifier (IC) in the second identifier (IA1) to be transmitted to the server resource (MS; SE), and the retrieval in the server resource includes application (E9) of the encrypted random number (RC) to the asymmetrical algorithm (AA) with the private key (KPR), in order to retrieve the generated random number (R), and application (E10) of the retrieved random number (R) as a key, and of the encrypted identifier (IC), to the symmetrical algorithm (AS), in order to retrieve the first identifier (ID).

4. A process in accordance with claim 1 or 2, according to which the determination in the terminal resource (TU, CP; PC, CA) includes application (E25) of the generated random number (R) and of the first identifier (ID), concatenated to the asymmetrical algorithm (AA) with the public key (KPU) to produce the second identifier (IA2) to be transmitted to the server resource (MS; SE), and the retrieval in the server resource includes application (E29) of the second identifier (IA2) to the asymmetrical algorithm (AA)

with the private key (KPR) in order to retrieve the first identifier (ID).

5. A process according to any of claims 1 to 4, which includes a change (E15; E35) of public key (KPU) and of private key (KPR) for the asymmetrical algorithm (AA) in the server resource (MS; SE) and downloading (E15; E35) of the changed public key (KPU) from the server resource to the terminal resource (TU, CP; PC, CA).

6. A process according to any of claims 1 to 5, according to which the generation of random number (E1) is periodic (E14; E34) in the terminal resource (TU, CP; PC, CA).

7. A process according to any of claims 1 to 6, according to which the generation of random number (E1) occurs (E14; E34) following at least one of the following events in the terminal resource (TU, CP; PC, CA): switching on of the terminal resource, setting-up of a call, setting-up of a session between the terminal resource and the server resource, substitution of the server resource for another server resource, or activation of a service application.

8. A user terminal resource (TU, CP; PC, CA) identifying itself, or identifying a user of the latter, to a server resource (MS; SE), through such a telecommunication network (RR; RT), using a first identifier (ID), an asymmetrical algorithm (AA) with a public key (KPU) being implemented in the terminal resource, characterised in that it includes:

- a resource (GA) to generate a random number (R), and

- a resource (PR, M1) to determine a second identifier (IA1; IA2) as a function of the random number, at least from part of the first identifier (ID) and from the result of executing the asymmetrical algorithm (AA) to which at least the random number is applied in order to transmit the second identifier (IA1; IA2) to the server resource (MS; SE), which retrieves the first identifier at least by executing the asymmetrical algorithm (AA) to which a private key (KPR) and, at least partially, the second identifier (IA1; IA2) are applied, and which verifies that the first retrieved identifier (ID) is written into a memory (HLR) of the server resource.

9. A user terminal resource according to claim 8, in which the resource to generate a random number (GA) and the resource to determine a second identifier (PR, M1) are included in a portable electronic object of the chip card type (CP; CA) .